Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Petition of American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties for a Declaratory Ruling to Interpret 47 U.S.C. § 333, or, in the Alternative, for Rulemaking	)	RM-11737

To: Chief, Consumer & Governmental Affairs Bureau

REPLY COMMENTS OF SMART CITY NETWORKS, LP

The comments filed to date in connection with the above-captioned petition for declaratory ruling[1] reinforce the fact, as pointed out in the comments made by Smart City Networks, LP ("Smart City"), that Section 333 of the Communications Act does not prohibit the use of standards-based containment measures, the targeted use of which is widespread around the world. Containment through de-authentication of harmful rogue Wi-Fi access points is recognized as a necessary tool to ensure the availability of unlicensed spectrum in highly congested environments that are not open to the public. The comments also confirm both the lack of Commission guidance regarding containment[2] and the need for the Commission to develop parameters that will permit reasonable Wi-Fi network management while continuing to

[1] Petition for Declaratory Ruling or, In the Alternative, For Rulemaking (filed by the American Hospitality & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties on Aug. 25, 2014 ("Petition"). *See* Public Notice, "Consumer & Governmental Affairs Bureau Reference Information Center, Petition for Rulemaking Filed," Rep. No. 3012 (rel. Nov. 19, 2014).

[2] The Enforcement Bureau based a recent enforcement action on the view that a particular instance of containment violates Section 333 (*see Marriott International, Inc. and Marriott Hotel Services, Inc.*, Order and Consent Decree, File No. EB-IHD-13-00011303, 29 FCC Rcd 11760 (EB, 2014) ("*Marriott Order and Consent Decree*"), but a consent decree of course is not precedent and provides no formal guidance from the Enforcement Bureau, let alone the Commission.

ensure that unlicensed spectrum generally is open and available for all who wish to make use of it.

I. Establishing Parameters For Reasonable Wi-Fi Network Management Would Not Create A *Carte Blanche* "Right To Interfere"

Parties opposing the Petition raise concerns that, read broadly, grant of the Petition would create a "carte blanche 'right to interfere'" with the operations of lawful devices operating on other Wi-Fi networks, particularly for unfair financial gain.[3] Smart City and others who support the Petition, however, are not advocating a "carte blanche 'right to interfere.'"[4] Indeed, most of the parties supporting the Petition seem to agree that devices in normal operation that do not pose a threat to security or to network reliability and that are operating in a public space should not be

[3] Comments of the Wireless Internet Service Providers Association, at 3 (filed Dec. 19, 2014) ("WISPA Comments"); *see also* Comments of CTIA – The Wireless Association, at 3 (filed Dec. 19, 2014) ("CTIA Comments") ("The Commission should therefore declare that the type of blanket de-authentication contemplated by the Petition violates the Act and the FCC's rules."); Opposition of the National Cable & Telecommunications Association, at 1 (filed Dec. 19, 2014) ("NCTA Opposition") ("In particular, the Hotel Interests seek the ability to disrupt the wireless communications of anyone whose Wi-Fi signal competes for spectrum with a venue-owner's own access points or otherwise behaves in a manner inconsistent with the owner's business objectives."); Opposition of Open Technology Institute at New America Foundation and Public Knowledge, at 2 (filed Dec. 19, 2014) ("Open Technology Opposition") ("As a matter of policy, Petitioner's proposed 'right to interfere' with Wi-Fi or other Part 15 operations undermines the public interest in multiple ways. First, Petitioner's proposed declaratory order is virtually boundless. It would open the door to the willful block or degrading of Wi-Fi by any venue that decided it could make a profit off its exclusive provision, or benefit in some other way by ensuring quality of service (QoS) for its own network."); Opposition of Google Inc., at 1 (filed Dec. 19, 2014) ("[W]hile Google recognizes the importance of leaving operators flexibility to manage their own networks, this does not include intentionally blocking access to other Commission-authorized networks, particularly where the purpose or effect of that interference is to drive traffic to the interfering operator's own network (often for a fee).").

[4] *See* Comments of Smart City Networks, LP (filed Dec. 19, 2014) ("Smart City Comments"); Comments of Cisco Systems, Inc., at 4 (filed Dec. 19, 2014) ("Cisco Comments") ("Cisco recognizes that operators of Wi-Fi networks should not have *carte blanche* to disrupt the operation of Wi-Fi or other unlicensed devices without legitimate justification."); Joint Comments of Aruba Networks, Inc. and Ruckus Wireless, Inc., at 11 (filed Dec. 19, 2014) ("Joint Comments") ("[T]he Commission will be taking on an obligation to engage in a careful balancing act, continuing to promote the widest possible use of Wi-Fi devices, while at the same time assuring that network administrators can protect their networks, data and customers from cybersecurity threats and from attempts to violate important network policies."); Comments of Hilton Worldwide Holdings Inc., at 1 (filed Dec. 19, 2014) ("Hilton Comments") ("In advocating that reasonable measures to address such congestion be allowed, Hilton is not seeking to prevent guests from making any use of person Wi-Fi access points on hotel property. . . .").

subject to containment.[5] These parties are urging the Commission to balance the public interest in protecting against carte blanche interference with the need for reasonable network management practices that ensure safe and reliable Wi-Fi service in non-public spaces and during private events.[6] The Commission can and should chart a course that advances both of these legitimate objectives.

Given the position taken by the Enforcement Bureau in the investigation the led to the *Marriott Order and Consent Decree*, and the $600,000 payment agreed to by Marriott to terminate that investigation, it is likely that many others who employ standards-based, FCC-certified equipment to contain "rogue" Wi-Fi access points have been deterred from filing comments in this proceeding for fear of being subjected to enforcement action. Nonetheless, the record in this proceeding amply demonstrates the need to ensure secure and reliable Wi-Fi service. The Joint Commenters, Cisco, and Hilton all provide information regarding the variety of cybersecurity threats faced by today's network operators. In addition, Smart City and other commenters demonstrate the need to manage networks to address network congestion and other challenges that can affect the reliability of Wi-Fi connectivity in circumstances in which private entities have reasonably come to expect the proper functioning of unlicensed services made available for their use.[7] As Cisco points out, a failure to acknowledge the legitimate use of standards-based network management tools such as de-authentication would essentially "de-value[] the use of Wi-Fi in enterprise and service provider environments, because the technology

[5] Smart City Comments at 12-14; Cisco Comments at 4; Hilton Comments at 4-11; Comments of the United States Telecom Association, at 2 (filed Dec. 22, 2014) ("USTelecom Comments").

[6] Smart City Comments at 12-14; Cisco Comments at 2-4; USTelecom Comments at 2-4; Hilton Comments at 4-11; Joint Comments at 11-12.

[7] *See* Smart City Comments at 2-7; USTelecom Comments at 1-4; Hilton Comments at 4-11.

at issue here is the same technology that protects Wi-Fi networks now [is] widespread throughout our economy."[8]

Smart City's comments demonstrated this general policy point in the real-world settings that exist today throughout the convention and trade show industry. Billions of dollars in business is conducted and concluded each year during convention and trade show events and reliable, high quality Wi-Fi service can mean the difference between success and failure for the participating parties as well as for the venues hosting these events. Convention exhibitors depend upon the availability of Wi-Fi to demonstrate and control products ranging from robotic and household appliances to medical devices and manufacturing equipment. Actual business transactions are being conducted wirelessly more and more in these venues, as well. Furthermore, reliable Wi-Fi connectivity is critical for the basic functioning of in-house services provided in convention venues themselves (e.g., food service point-of-sale and credit card verification systems), as well as for internal building systems used in venues operations (e.g., wireless ticket readers, etc.). As a consequence, to provide secure, reliable Wi-Fi service during convention events, network providers throughout the world have developed global industry standards and best practices that enable them to manage wireless networks and ensure uninterrupted connectivity inside these proprietary spaces. Primary among these network management tools is Wi-Fi de-authentication using standards-based equipment that has been certified by the FCC.[9]

Smart City's comments further showed how access to unlicensed spectrum resources can be reasonably balanced against the need to protect networks from cybersecurity threats and to

[8] Cisco Comments at 3.

[9] As Smart City has pointed out, international venue managers attending the annual conference of the International Association of Convention Centres (http://www.aipc.org/) in Berlin last summer confirmed the widespread use of containment features to control their venues' wireless environments.

provide reliable service in congested environments. Essentially, to distinguish between acceptable and unacceptable uses of de-authentication technology, the Commission should consider the purpose for which containment is being used, the location in which containment is being used, and whether containment is based upon standards reasonably tailored to suit the purpose for containment.

For instance, in those cases in which Smart City has used de-authentication in the past,[10] it targeted only access points and wireless devices that are located within the confined and proprietary space of the exhibit hall – areas of a convention center that are licensed for a private event and to which access is limited – and that pose a threat to secure, reliable Wi-Fi availability within that confined space.[11] The need for reliable access is most critical inside exhibit halls where convention exhibitors demonstrate their products and services. At the same time, unauthorized access points or wireless devices are most likely to degrade network reliability in these spaces, making the need to engage in responsible wireless network management most critical there as well.

The Commission can employ an objective measure – such as the Relative Signal Strength Indicator ("RSSI") level that Smart City has used in the past – as the standard for identifying and containing unauthorized access points that pose an imminent threat to the security and/or reliability of the Wi-Fi environment. In this way, de-authentication is targeted only to those access points and wireless devices that actually may impair the throughput and

[10] Smart City has not used de-authentication in the majority of the convention venues that it serves and, in light of the recent *Marriott Order and Consent Decree*, it has discontinued the use of de-authentication in those venues where it did use this technology.

[11] It is important to note that a typical convention venue includes both public spaces, where any person can enter without a ticket, and private spaces such as exhibit halls, which allow entry only by authorized persons who essentially have purchased or been granted licenses to enter proprietary space, which typically include restrictions on permissible activities while in that space. Smart City regularly provides free Wi-Fi service in the public, non-exhibition, spaces.

reliability of the Wi-Fi network in the exhibit hall. This approach does not implicate the concerns of "blanket" de-authentication that some commenters have raised, but instead targets containment efforts to circumstances in which they are necessary to allow the vast majority of Wi-Fi users to reliably connect.[12] Used in this way, de-authentication imposes only a minimal burden on those who wish to use Wi-Fi access points and other wireless devices in an exhibit hall or other proprietary space, while serving the critical goal of maintaining a secure and reliable Wi-Fi network for the vast majority of users there.

II. Section 333 Cannot Be Read To Bar Wi-Fi Containment

Some commenters have argued that Section 333 of the Communications Act of 1934, 47 U.S.C. § 333, stands as a general bar to the use of containment measures – even the kinds of reasonable network management approaches Smart City advocates – and that the Commission therefore cannot grant the Petition.[13] This is not the case. Commenters arguing in favor of this interpretation of Section 333 fail to provide any compelling rationale under which the Commission could legally conclude that unlicensed wireless devices are "radio stations" covered by Section 333.

Nor do these parties adequately demonstrate that use of standards-based management tools like de-authentication constitutes "interference," which is "[t]he effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system …."[14] As the Joint Comments demonstrate, de-authentication "does not increase the undesired signal level or otherwise cause electromagnetic interference …. It is

[12] As employed by Smart City in the past, the RSSI metric allowed unauthorized access points or devices to avoid de-authentication simply by moving a few steps in one direction or another.

[13] *Compare* WISPA Comments; CTIA Comments; NCTA Opposition; Open Technology Opposition; Google Opposition *with* Smart City Comments; Cisco Comments; Joint Comments; Hilton Comments.

[14] 47 C.F.R. § 2.1.

the way the ... device interprets the de-authentication frame, not the RF characteristics of the signal that leads the device to discontinue communications."[15] For these same reasons, commenters opposing the Petition have not demonstrated that de-authentication as an 802.11-based network management technology constitutes "jamming" that is prohibited by Section 333.[16]

This is not to say that the Commission lacks statutory authority to regulate the use of de-authentication so that Wi-Fi network operators do not have or exercise carte blanche interference rights. Indeed, Section 302 of the Act provides adequate legal authority for the Commission to ensure that unlicensed spectrum generally is open and available for all who wish to make use of it.[17] The parties favoring the Petition are merely asking the Commission to exercise this authority in a targeted way that acknowledges the value and fundamental reasonableness of standards-based network management practices, including de-authentication technology, used to protect Wi-Fi networks from security threats and to ensure the provision of reliable service in certain instances.

For the reasons set forth herein and in Smart City's comments, the Commission should issue a declaratory ruling making clear that the use of de-authentication measures by a Wi-Fi network operator using Commission-authorized equipment to manage its network on its own

---

[15] Joint Comments at 7. Smart City, USTelecom and Cisco also have shown that 802.11-based network management technologies do not involve "interference" under Section 333. *See* Cisco Comments at 3; USTelecom Comments at 2-3; Smart City Comments at 7-11.

[16] A Feb. 9, 2011 Enforcement Bureau advisory warned against the use of "cell and GPS jammers that could not be legally sold in the United States (*see* FCC Enforcement Advisory, *Cell Jammers, GPS Jammers, and Other Jamming Devices*, 26 FCC Rcd 1329 (2011)), and the Commission has taken action against the illegal marketing of signal jammers that "have no lawful consumer use in the United States" (*see C.T.S. Technology Co.*, Notice of Apparent Liability for Forfeiture and Order, 29 FCC Rcd 8107 (2014)). Neither of these actions can reasonably be viewed as a warning against the use of de-authentication technology included in FCC-certified, legally marketed 802.11 standard-based devices.

[17] *See, e.g.,* Smart City Comments at 9.

premises does not violate Section 333 of the Act. The Commission also could, if it chooses to, provide appropriate guidance as to how de-authentication may be used consistent with the public interest and Part 15 of the Commission's rules.

Respectfully submitted,

SMART CITY NETWORKS, LP

By: /s/ *Mark Haley*
Mark Haley, President

SMART CITY NETWORKS, LP
5795 W. Badura Ave., Suite 110
Las Vegas, NV 89118
(702) 943-6000

January 5, 2015